



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,126	07/11/2001	Christian Wettergren	64591-64607-EN/CMN	8110

466 7590 09/14/2005

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,126	WETTERGREN, CHRISTIAN	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 9-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 9-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 7/1/2005.

2 **DETAILED ACTION**

3 ***Continued Examination Under 37 CFR 1.114***

4 A request for continued examination under 37 CFR 1.114, including the fee set forth in
5 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is
6 eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)
7 has been timely paid, the finality of the previous Office action has been withdrawn pursuant to
8 37 CFR 1.114. Applicant's submission filed on 7/1/2005 has been entered.

9 ***Response to Arguments***

10 Applicant argues primarily that Francisco did not disclose the security processor
11 executing the critical activity.

12 Applicant's arguments with respect to claim 9-16 have been considered but are moot in
13 view of the new ground(s) of rejection.

14 Claims 1-8 have been canceled.

15 Claims 9-16 have been examined

16 All objections and rejections not set forth below have been withdrawn.

17 ***Claim Rejections - 35 USC § 112***

18 The following is a quotation of the second paragraph of 35 U.S.C. 112:

19 The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
20 subject matter which the applicant regards as his invention.

21
22 Claims 9-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for
23 failing to particularly point out and distinctly claim the subject matter which applicant regards as
24 the invention.

Claim 9 recites the limitation "the computer processor" in lines 15-16, 18-19, and 23, as well as claim 13 lines 3-4. There is insufficient antecedent basis for this limitation in the claim. The examiner will assume for purposes of applying prior art that this limitation was meant to refer to the processor in the computer, and not the processor in the security device.

Claim 15 recites the limitation "the content" in line 36. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

Regarding claim 9, Francisco disclosed a system for data processing a security critical activity in a secure management mode in a computer (See Francisco Abstract Lines 6-10), which computer comprises a processor (See Francisco Fig. 1 Element 1), handling devices (See Francisco Fig. 1 Element 25), memory storage means (See Francisco Fig. 1 Element 30), hereafter named resources; that the system comprises a security device (See Francisco Fig. 1 Elements 31 and 100) comprising a processor (See Francisco Fig. 1 Element 7) and signal generators (See Francisco Fig. 3 Element 321), a number of control means, hereafter named switches (See Francisco Fig. 3 Element 325), with signal receivers (See Francisco Col. 5

Art Unit: 2131

Paragraph 6 wherein it was inherent that the AMU control had signal generators and the AMU had signal receivers in order for the Control to have configured the AMU) arranged respectively between the security device and the pre-selected resources (See Francisco Fig. 1 Elements 31, 100, and 30), that the switches contain information regarding accessibility to and from the resources, or parts of the resources, hereafter named resource ranges (See Francisco Fig. 1 Element 102 and Claims 1-2), characterized in that the switch controls requests from the computer processor to the resources or resource ranges depending on the information contained in the switch (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2), and that in response to a call from the computer processor or the handling devices, the switches are activated by receiving a signal from the security device, enabling the security device access to and from the resources or resource ranges selected by the security device, and denying the computer processor access to and from the resources or resource ranges selected by the security device (See Francisco Col. 4 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject is denied access when they are requesting an access outside the subjects access rights), in that the signal (SG_{PM}) can be generated only by the security device (See Francisco Col. 5 Paragraph 6 Lines 1-4), and in that the security device comprises a signal generator (SG_A), wherein, when a switch receives a signal (SG_A), together with new information (addresses, operation, data), the security device is able of altering the content of the information of that switch (See Francisco Col. 5 Lines 39-50), but Francisco failed to disclose that the security device processor had access to the resources or the security device processor executed the security critical activity.

1 Clifton teaches that in a computing system it is desirable to have classify certain
2 instructions as secure and others as unsecure and to have a normal processor execute the
3 unsecure instructions and a secure processor to processor to execute the secure instructions (See
4 Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

5 It would have been obvious to the ordinary person skilled in the art at the time of
6 invention to employ the teachings of Clifton in the personal computer security system of
7 Francisco by classifying certain instructions as secure and only allowing the secure instructions
8 to be executed by the security processor. This would have been obvious because the ordinary
9 person skilled in the art would have been motivated to protect against the destruction of
10 important data and the compromise of secret or confidential data.

11 Regarding claim 15, Francisco disclosed a system for data processing a security critical
12 activity in a secure management mode in a computer (See Francisco Abstract Lines 6-10),
13 comprising: a computer comprising a computer processor (See Francisco Fig. 1 Element 1),
14 handling devices (See Francisco Fig. 1 Element 25), memory storage resources (See Francisco
15 Fig. 1 Element 30); a security device (See Francisco Fig. 1 Elements 31 and 100) comprising
16 security device processor (See Francisco Fig. 1 Element 7) and signal generators (See Francisco
17 Fig. 3 Element 321) inputting into the security device processor (See Francisco Col. 2 Lines 22-
18 29 and Col. 5 Paragraph 6); and switch control means (See Francisco Fig. 3 Element 325)
19 comprising switches and signal receivers (See Francisco Col. 5 Paragraph 6 wherein it was
20 inherent that the AMU control had signal generators and the AMU had signal receivers in order
21 for the Control to have configured the AMU), the switches of the switch control means arranged
22 respectively between the security device and pre-selected memory storage resources (See

Art Unit: 2131

1 Francisco Fig. 1 Elements 31, 100, and 30), wherein, the switches of the switch control means
2 contain information regarding accessibility to and from the memory storage resources, or ranges
3 within the memory storage resources (See Francisco Fig. 1 Element 102, and Claims 1-2), the
4 switch control means, depending on the information contained in the switches, controls requests
5 from the computer processor to the memory storage resources or ranges within the memory
6 storage resources (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2),
7 and in response to a call from the computer processor or the handling devices, the switches are
8 activated receiving a control signal from the security device and the security device processor, i)
9 enabling the security device access to and from the memory storage resources or the ranges
10 within the switch control means memory storage resources selected by the security device and ii)
11 denying the computer processor access to and from the memory storage resources or the ranges
12 within the memory storage resource selected by the security device (See Francisco Col. 4
13 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject
14 is denied access when they are requesting an access outside the subjects access rights), the
15 control signal (SGPM) can be generated only by the security device (See Francisco Col. 5
16 Paragraph 6 Lines 1-4), upon any switch receiving a signal (SGA), together with new
17 information (addresses, operation, data), the security device configured to alter the content of the
18 information of that switch (See Francisco Col. 5 Lines 39-50), and the security device processor
19 is a different processor than the computer processor (See Francisco Fig. 1 Elements 1 and 7), but
20 Francisco failed to disclose that the security device processor had access to the resources or the
21 security device processor executed the security critical activity.

1 Clifton teaches that in a computing system it is desirable to have classify certain
2 instructions as secure and others as unsecure and to have a normal processor execute the
3 unsecure instructions and a secure processor to processor to execute the secure instructions (See
4 Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

5 It would have been obvious to the ordinary person skilled in the art at the time of invention to
6 employ the teachings of Clifton in the personal computer security system of Francisco by
7 classifying certain instructions as secure and only allowing the secure instructions to be executed
8 by the security processor. This would have been obvious because the ordinary person skilled in
9 the art would have been motivated to protect against the destruction of important data and the
10 compromise of secret or confidential data.

11 Regarding claim 16, Francisco disclosed a system for data processing a security
12 critical activity in a secure management mode in a computer (See Francisco Abstract Lines 6-
13 10), comprising: a computer comprising a computer processor (See Francisco Fig. 1 Element 1),
14 connected to handling devices (See Francisco Fig. 1 Element 25) and to memory storage
15 resources (See Francisco Fig. 1 Element 30); a security device (See Francisco Fig. 1 Elements 31
16 and 100) comprising a security device processor (See Francisco Fig. 1 Element 7) and signal
17 generators (See Francisco Fig. 3 Element 321) inputting into the security device processor (See
18 Francisco Col. 2 Lines 22-29 and Col. 5 Paragraph 6); and switch control means (See Francisco
19 Fig. 3 Element 325) comprising switches and signal receivers (See Francisco Col. 5 Paragraph 6
20 wherein it was inherent that the AMU control had signal generators and the AMU had signal
21 receivers in order for the Control to have configured the AMU), the switches of the switch
22 control means arranged between the security device and pre-selected memory storage resources

(See Francisco Fig. 1 Elements 31, 100, and 30), wherein, the switches of the switch control means contain information regarding accessibility to and from the memory storage resources, (See Francisco Fig. 1 Element 102, and Claims 1-2), the switch control means, based on the information contained in the switches, controls requests from the computer processor to the memory storage resources (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2), and in response to a call from the computer processor, the switches are activated by receiving a control signal from the security device and the security device processor to i) enable the security device access to and from the memory storage resources selected by the security device and ii) deny the computer processor access to and from the memory storage resources selected by the security device (See Francisco Col. 4 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject is denied access when they are requesting an access outside the subjects access rights), the control signal (SGPM) can be generated only by the security device (See Francisco Col. 5 Paragraph 6 Lines 1-4), upon any switch receiving a signal (SGA), together with new information (addresses, operation, data), the security device configured to alter the content of the information of that switch (See Francisco Col. 5 Lines 39-50), and the security device processor is a different processor than the computer processor (See Francisco Fig. 1 Elements 1 and 7), but Francisco failed to disclose that the security device processor had access to the resources or the security device processor executed the security critical activity.

Clifton teaches that in a computing system it is desirable to have classify certain instructions as secure and others as unsecure and to have a normal processor execute the

1 unsecure instructions and a secure processor to processor to execute the secure instructions (See
2 Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

3 It would have been obvious to the ordinary person skilled in the art at the time of invention to
4 employ the teachings of Clifton in the personal computer security system of Francisco by
5 classifying certain instructions as secure and only allowing the secure instructions to be executed
6 by the security processor. This would have been obvious because the ordinary person skilled in
7 the art would have been motivated to protect against the destruction of important data and the
8 compromise of secret or confidential data.

9 Regarding claim 10, the combination of Francisco and Clifton disclosed that the
10 information contained in the switches controls access to resources for requests from other
11 possible processors contained in or connected to the computer (See Francisco Col. 6 line 68 –
12 Col. 7 Line 4).

13 Regarding claim 11, the combination of Francisco and Clifton disclosed that the switches
14 comprise a signal receiver by which it can detect which source is handling the computer, and that
15 the switch compares this with the resource which requests access to a resource or resource range
16 controlled by the switch, and depending on the information in the switch, enables or denies
17 access to that resource (See Francisco Fig. 2b).

18 Regarding claim 12, the combination of Francisco and Clifton disclosed that the
19 information in the switch enables the switch to control certain areas of the memory means are
20 allocated to be accessed by the processor of the security device only (See Francisco Col. 4
21 Paragraph 3).

1 Regarding claim 13, the combination of Francisco and Clifton disclosed that the
2 information in the switch enables the switch to control that certain resources are accessible by
3 the computer processor when not in secure management mode, and only accessible by the
4 security device when in secure management mode (See Francisco Col. 2 paragraph 3 wherein the
5 large address space mode constituted the non-secure mode and the segmented address space
6 constituted the secure mode).

7 Regarding claim 14, the combination of Francisco and Clifton disclosed that the switches
8 are hardware switches (See Francisco Fig. 4 Element 325).

9

Art Unit: 2131

Conclusion


Claims 1-8 have been have been canceled and claims 9-16 have been rejected..


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew Henning
Assistant Examiner
Art Unit 2131
9/7/2005


Primary Examiner
AU2131
9/9/05